

Improved Eavesdropping Detection Strategy in Quantum Direct Communication Protocol Based on Four-particle GHZ State

Li Jian¹, Jin Haifei^{1,*}, Jing Bo^{1,2}

¹ *School of Computer, Beijing University of Posts and Telecommunications,
Beijing 100876, People's Republic of China*

² *Department of Computer Science, Beijing Institute of Applied Meteorology,
Beijing 100029, People's Republic of China*

Abstract

In order to improve the eavesdropping detection efficiency in two-step quantum direct communication protocol, an improved eavesdropping detection strategy using four-particle GHZ state is proposed, in which four-particle GHZ state is used to detect eavesdroppers. During the security analysis, the method of the entropy theory is introduced, and two detection strategies are compared quantitatively by using the constraint between the information which eavesdropper can obtain and the interference introduced. If the eavesdroppers intend to obtain all information, the eavesdropping detection rate of the original two-step quantum direct communication protocol by using EPR pair block as detection particles is 50%; while the proposed strategy's detection rate is 88%. In the end, the security of the proposed protocol is discussed. The analysis results show that the eavesdropping detection strategy presented is more secure.

Keywords: quantum direct communication; four-particle GHZ state; eavesdropping detection; protocol security; dense coding scheme

PACS: 03.67.Hk, 03.65.Ud, 03.67.Dd, 03.65.Ta

1 Introduction

The goal of cryptography is to ensure that the secret message is intelligible only for the two authorized parties of communication and should not be altered during the transmission. So far, it is trusted that the only proven secure cryptophyte is the one-time-pad scheme in which the secret key is as long as the

* E-mail:jinhaifei@bupt.edu.cn

message. The two distant parties who want to transmit their secret message must distribute the secret key first. But it is difficult to distribute securely the secret key through a classical channel. The quantum key distribution (QKD), whose task is to create a secret key between two remote authorized users, is one of the most remarkable applications of quantum mechanics and the only proven protocol for secure key distribution. Since Bennet and Brassard presented the pioneer QKD protocol (BB84 protocol) [1] in 1984, a lot of quantum information security processing methods have been advanced, such as quantum teleportation [2-7], quantum dense coding [8-9], quantum secret sharing [10-11] and so on.

In recent years, a novel concept, quantum secure direct communication (QSDC) was put forward and studied by some groups. Different from key distribution whose object is to establish a common random key between two parties, a secure direct communication is to communicate important message directly without first establishing a random key to encrypt them. Thus secure direct communication is more demanding on the security. As a secure direct communication, it must satisfy two requirements. First, the secure message should be read out directly by the legitimate user Bob when he receives the quantum state and no additional classical information is needed after the transmission of particles. Second, the secret message which has been encoded already in the quantum states should not leak even though an eavesdropper may get hold of the channel. That is to say, the eavesdropper cannot only be detected but also obtains blind results. As classical message can be copied fully, it is impossible to transmit secret message directly through classical channels. But when quantum mechanics enters into the communication, the story will change.

Another class of quantum communication protocols [12-14] used to transmit secret message are called deterministic secure quantum communication (DSQC). Certainly, the receiver can read out the secret message only after he exchanges at least one bit of classical information for each particle with the sender in a DSQC protocol, which is different from QSDC. DSQC is similar to QKD, but it can be used to obtain deterministic information, not a random binary string, which is different from the QKD protocols in which the user cannot predict whether an instance is useful or not.

Many people are interested in researching QSDC, and many protocols like QSDC were proposed, including the protocols without using entanglement [15-17], the protocols using entanglement [18-23] and the two-way QSDC protocols [24-33]. The QSDC protocol can also be used in some special environments as first proposed by Boström et al. [34] and Deng et al. [18]. In Ref. [34], Bostrom and Felbinger presented a famous QSDC protocol which is called "ping-pong" protocol. But researchers have found much vulnerability in the "ping-pong" protocol, such as the "ping-pong" protocol cannot resist the "man-in-middle attack" and the transmission capacity is low.

In order to improve the eavesdropping detection efficiency in two-step quantum direct communication protocol, an improved eavesdropping detection

strategy using four-particle GHZ state is proposed, in which four-particle GHZ state is used to detect eavesdroppers. During the security analysis, the method of the entropy theory is introduced, and two detection strategies are compared quantitatively by using the constraint between the information which eavesdropper can obtain and the interference introduced. If the eavesdroppers intend to obtain all information, the eavesdropping detection rate of the original two-step quantum direct communication protocol by using EPR pair block as detection particles is 50%; while the proposed strategy's detection rate is 88%. In the end, the security of the proposed protocol is discussed. The analysis results show that the eavesdropping detection strategy presented is more secure.

For simplicity, suppose that the protocol presented in Ref. [18] is shortened as DPP and the improved protocol in this paper is shortened as FPP.

2 DPP Protocol

An EPR pair can be in one of the four Bell states,

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \quad (1)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad (2)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad (3)$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (4)$$

If the state of a single photon be measured, the Bell state will collapse and the state of the other particle will be completely determined if we know the measurement result of the first photon. As is known to all, the basic principle of the original "ping-pong" protocol is that one bit information can be encoded in the states $|\psi^\pm\rangle$, which is completely unavailable to anyone who has access to either of the particles. To extract secret message from Alice, Bob must own both particles, for no experiment performed on only one particle can distinguish these states from each other [34].

Let us start with a brief description of the DPP protocol.

(S1) Alice prepares an ordered N EPR pairs in state $|\psi^-\rangle$, extracts all the first particles, and forming the sequence S_1 in order. The remainder particles are formed the sequence S_2 in order.

(S2) Alice sends the sequence S_1 to Bob. Alice and Bob then check eavesdropping by the following procedure: (a) Bob chooses randomly a number of the photons from the sequence S_1 and tells Alice which particles he has chosen. (b) Bob chooses randomly one of the two sets of MBs, say, σ_Z and σ_X to

measure the chosen photons. (c) Bob tells Alice which MB he has chosen for each photon and the outcomes of his measurements. (d) Alice uses the same MB as Bob to measure the corresponding photons in the sequence S_2 and checks with the results of Bob. If no eavesdropper exists, their results should be completely opposite. This is the first eavesdropping check. After that, if the error rate is small, Alice and Bob can conclude that there is no eavesdropper in the line. Alice and Bob continue to perform step(S3); otherwise, they have to discard their transmission and abort the communication.

(S3) Alice encodes her messages on the sequence S_2 and transmits it to Bob. Before the transmission, Alice must encode the EPR pairs. In order to guard for eavesdropping in this transmission, Alice has to add a small trick in the sequence S_2 . She selects randomly in the sequence S_2 some particles and performs on them randomly one of the four operations. The number of such particles is not big as long as it can provide an analysis of the error rate. Only Alice knows the positions of these sampling particles and keeps them secret until the communication is completed. The remaining sequence S_2 particles are used to carry the secret message directly. To encode the message, they use the dense coding scheme of Bennett and Wiesner [8], where the information is encoded on an EPR pair with a local operation on a single qubit. Here, the dense coding idea was generalized into secure direct communication. Different from dense coding, in this protocol, both the particles in an EPR pair are sent from Alice to Bob in two steps, and the transmission of EPR pairs is done in block. Explicitly, Alice makes one of the four unitary operations (U_0, U_1, U_2 and U_3) to each of her particles,

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad (5)$$

$$U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad (6)$$

$$U_2 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad (7)$$

$$U_3 = -i\sigma_y = |1\rangle\langle 0| - |0\rangle\langle 1|. \quad (8)$$

And they transform the state $|\psi^-\rangle$ into $|\psi^-\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$ and $|\phi^+\rangle$, respectively. These operations correspond to 00, 01, 10 and 11, respectively.

(S4) After the transmission of sequence S_2 , Alice tells Bob the positions of the sampling pairs and the type of the unitary operations on them. Bob performs Bell-basis measurement on the sequence S_1 and S_2 simultaneously. By checking the sampling pairs that Alice has chosen, he will get an estimate of the error rate in the sequence S_2 transmission. In fact, in the second transmission, Eve can only disturb the transmission and cannot steal the information because she can only get one particle from an EPR pair.

(S5) If the error rate of the sampling pairs is reasonably low, Alice and Bob can then entrust the process, and continue to correct the error in the secret message using error correction methods. Otherwise, Alice and Bob abandon the transmission and repeat the procedure from the beginning.

(S6) Alice and Bob do error correction on their results. This procedure is exactly the same as that in QKD. However, to preserve the integrity of the message, the bits preserving correction code, such as CASCADE [35], should be used.

3 FPP Protocol

3.1 The process of the FPP protocol

In the protocol presented in Ref.[36], the transmission is managed in batches of N EPR pairs. An advantage of block transmission scheme is that we can check the security of the transmission by measuring some of the decoy photons [37-38] in the first step, where both Alice and Bob contain a particle sequence at hand, which means that an eavesdropper has no access to the first particle sequence, then no information will be leaked to her whatever she has done to the second particle sequence. Following this method using block transmission, the FPP scheme is proposed, shown in Fig.1.

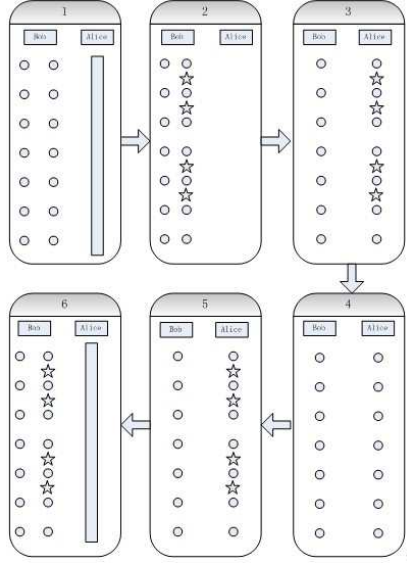


Fig. 1. The process of the FPP

Define

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle). \quad (9)$$

Now let us give an explicit process for the FPP.

(S1) Bob prepares a large enough number (N) of Bell states $|\phi^+\rangle$ in order. He

extracts all the first particles in these Bell state, forming the sequence A (*the travel qubits*) in order, used to transmit secure message, and the remaining particles forming the sequence B (*the home qubits*) in order.

(S2) Bob prepares a large number ($cN/(1-c)$) of four-particle GHZ states $|\psi\rangle$ and forms the sequence C to detect eavesdropping. Here, c expresses the probability of switching to the control mode in the original "ping-pong" protocol [34]. Note that the sequence C includes $4cN/(1-c)$ particles. In the sequence C , Bob reserves the particle 1 of the four-particle GHZ state, and measures them by Z-basis $B_Z = \{|0\rangle, |1\rangle\}$. After that, Bob inserts particles 2, 3, 4 of the four-particle GHZ state to the sequence A randomly, forming a new sequence D , which includes decoy photons of four-particle GHZ state, but only Bob knows the position of decoy photons.

(S3) Bob stores the sequence B and sends the sequence D to Alice.

(S4) After Alice received the sequence D , Bob tells her the positions where are the decoy photons and the measurement of particles 1 of four-particle GHZ state in C . Then, Alice extracts the decoy photons from the sequence D and performs measurement. This is the first eavesdropping check. If there is no eavesdropper, when Bob's measurement is $|0\rangle$, then the measurement result of particles 2, 3, 4 should be $|000\rangle$; while Bob's measurement is $|1\rangle$, particles 2, 3, 4 should be $|111\rangle$, and they continue to the next step (S5), the FPP protocol keeping on. Otherwise, the communication is interrupted, and the FPP protocol switches to (S1).

(S5) Alice discards the decoy photons, then the sequence D becomes to the sequence A again. Alice encodes her messages on the sequence A and transmits it to Bob. In order to guard for eavesdropping in this transmission, Alice also has to insert some four-particle GHZ state particles in the sequence A before the transmission. Alice only inserts particles 2, 3, 4 of the four-particle GHZ state in the sequence A and reserves the particle 1. Only Alice knows the positions of these decoy photons and the measurement results of the particles 1, and keeps them until the communication is completed. The sequence A are used to carry the secret message directly. To increase the transmission capacity, the dense coding scheme be used to encode the secret message. Different from dense coding, in this protocol, the transmission of EPR pairs is done in block. Explicitly, Alice makes one of the four unitary operations (U_0, U_1, U_2 and U_3) to each of her particles, and they transform the state $|\phi^+\rangle$ into $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$, respectively. These operations correspond to 00, 01, 10 and 11, respectively. Then Alice transmits the sequence A which carries decoy photons to Bob.

(S6) After transmitting the sequence A , Alice tells Bob the positions of the decoy photons and the measurement results of the particles 1. To obtain the secret message, Bob performs Bell-basis measurement on the sequences A and B simultaneously. By checking the decoy photons that Alice insert, Bob will get an estimate of the error rate in the sequence A transmission. In fact, Eve

can only disturb the transmission and cannot steal the information because she can only get one particle from an EPR pair. If the error rate of the decoy photons is reasonably low, Alice and Bob can then entrust the process, and continue to transmit the secret message. Otherwise, Alice and Bob abandon the transmission and repeat the procedures from the beginning.

As discussed above, the secret message can be transmitted securely between Alice and Bob, and the eavesdropper will be found out if she disturbs the quantum line. Eve cannot read out the information from the EPR pairs even if she captures the sequence A , because no one can read the information from one particle of the EPR pair alone. So, the improved protocol is secure.

3.2 The security analysis of the protocol

In the original "ping-pong" protocol, the author calculated the maximal amount of the information $I(d_{lO})$ that Eve can eavesdrop and the probability d_{lO} that Eve is detected [34]. And the function $I(d_{lO})$ is provided. When $p_0 = p_1 = 0.5$,

$$I(d_{lO}) = -d_{lO}\log_2 d_{lO} - (1 - d_{lO})\log_2(1 - d_{lO}). \quad (10)$$

The above method can be used to compare the efficiency of eavesdropping detection between the two protocols.

Now, let us analyze the efficiency of eavesdropping detection in FPP protocol. In order to gain the information that Alice operates on *the travel qubits*, Eve performs the unitary attack operation E on the composed system firstly. Then Alice takes a coding operation on *the travel qubits*. Eve performs a measurement on the composed system at last. Note that, all transmitted particles are sent as block before detecting eavesdropping, which is different from the original "ping-pong" protocol. For Eve does not know which particles are used to detect eavesdropping, so what she can do is only performing the same attack operation on all the particles. As for Eve, the state of *the travel qubits* is indistinguishable from the complete mixture, so all *the travel qubits* are considered in either of the states $|0\rangle$ or $|1\rangle$ with equal probability $p = 0.5$.

Generally speaking, suppose there is a group of decoy photons at the four-particle GHZ state $|\psi\rangle$, and after performed the attack operation E , the states $|0\rangle$ and $|1\rangle$ become

$$|\varphi'_0\rangle = E \otimes |0x\rangle = \alpha|0x_0\rangle + \beta|1x_1\rangle, \quad (11)$$

$$|\varphi'_1\rangle = E \otimes |1x\rangle = m|0y_0\rangle + n|1y_1\rangle, \quad (12)$$

where $|x_i\rangle$ and $|y_i\rangle$ are the pure ancillary states determined by the operation E uniquely, and

$$|\alpha|^2 + |\beta|^2 = 1, |m|^2 + |n|^2 = 1. \quad (13)$$

Then let us calculate the detection probability. Attacked by Eve, the state of composed system becomes

$$\begin{aligned}
|\psi\rangle_{Eve} &= I \otimes E \otimes E \otimes E \left[\frac{1}{\sqrt{2}} (|0x0x0x0x\rangle + |1x1x1x1x\rangle) \right] \\
&= \frac{1}{\sqrt{2}} [|0\rangle \otimes (\alpha|0x_0\rangle + \beta|1x_1\rangle) \otimes (\alpha|0x_0\rangle + \beta|1x_1\rangle) \otimes (\alpha|0x_0\rangle + \beta|1x_1\rangle) \\
&\quad + |1\rangle \otimes (m|0y_0\rangle + n|1y_1\rangle) \otimes (m|0y_0\rangle + n|1y_1\rangle) \otimes (m|0y_0\rangle + n|1y_1\rangle)] \\
&= \frac{1}{\sqrt{2}} [|0\rangle \otimes (\alpha^3|0x_00x_00x_0\rangle + \alpha^2\beta|0x_00x_01x_1\rangle + \alpha^2\beta|0x_01x_10x_0\rangle + \alpha\beta^2|0x_01x_11x_1\rangle \\
&\quad + \alpha^2\beta|1x_10x_00x_0\rangle + \alpha\beta^2|1x_10x_01x_1\rangle + \alpha\beta^2|1x_11x_10x_0\rangle + \beta^3|1x_11x_11x_1\rangle) \\
&\quad + |1\rangle \otimes (m^3|0y_00y_00y_0\rangle + m^2n|0y_00y_01y_1\rangle + m^2n|0y_01y_10y_0\rangle + mn^2|0y_01y_11y_1\rangle \\
&\quad + m^2n|1y_10y_00y_0\rangle + mn^2|1y_10y_01y_1\rangle + mn^2|1y_11y_10y_0\rangle + n^3|1y_11y_11y_1\rangle)]. \quad (14)
\end{aligned}$$

Obviously, when Alice performs measurement on the decoy photons, the probability without eavesdropper is

$$p(|\psi\rangle_{Eve}) = \frac{1}{2}(|\alpha^3|^2 + |n^3|^2). \quad (15)$$

So the lower bound of the detection probability is

$$d_{lF} = 1 - p(|\psi\rangle_{Eve}) = 1 - \frac{1}{2}(|\alpha^3|^2 + |n^3|^2). \quad (16)$$

Suppose $|\alpha|^2 = a$, $|\beta|^2 = b$, $|m|^2 = s$, $|n|^2 = t$, where a, b, s and t are positive real numbers, and $a + b = s + t = 1$. Then

$$d_{lF} = 1 - \frac{1}{2}(a^3 + t^3). \quad (17)$$

However, in DPP, authors calculated the efficiency of eavesdropping detection, here don't analyze it again, and the efficiency is

$$d_{lD} = |\beta|^2 = |\beta'|^2 = 1 - |\alpha|^2 = 1 - |\alpha'|^2. \quad (18)$$

Now, let us analyze how much information Eve can gain maximally when there is no control mode. Similar to that in Ref. [18], first, let us suppose that the quantum state of the photon in the hand of Alice is $|0\rangle$, Alice takes measurement on the photon in her hand with single-photon detector and the state is $|0\rangle$. Then the state of the system composed of Bob's photon is

$$|\psi'\rangle = E|0, E\rangle \equiv E|0\rangle|E\rangle = \alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle \equiv \alpha|0, \varepsilon_{00}\rangle + \beta|1, \varepsilon_{01}\rangle, \quad (19)$$

and Eve's probe can be described by

$$\rho' = |\alpha|^2 |0, \varepsilon_{00}\rangle \langle 0, \varepsilon_{00}| + |\beta|^2 |1, \varepsilon_{01}\rangle \langle 1, \varepsilon_{01}| + \alpha\beta^* |0, \varepsilon_{00}\rangle \langle 1, \varepsilon_{01}| + \alpha^*\beta |1, \varepsilon_{01}\rangle \langle 0, \varepsilon_{00}|. \quad (20)$$

After encoding of the unitary operations U_0, U_1, U_2 and U_3 with the probabilities p_0, p_1, p_2 and p_3 , respectively, the state reads

$$\begin{aligned} \rho'' = & (p_0 + p_3) |\alpha|^2 |0, \varepsilon_{00}\rangle \langle 0, \varepsilon_{00}| + (p_0 + p_3) |\beta|^2 |1, \varepsilon_{01}\rangle \langle 1, \varepsilon_{01}| \\ & + (p_0 - p_3) \alpha\beta^* |0, \varepsilon_{00}\rangle \langle 1, \varepsilon_{01}| + (p_0 - p_3) \alpha^*\beta |1, \varepsilon_{01}\rangle \langle 0, \varepsilon_{00}| \\ & + (p_1 + p_2) |\alpha|^2 |1, \varepsilon_{00}\rangle \langle 1, \varepsilon_{00}| + (p_1 + p_2) |\beta|^2 |0, \varepsilon_{01}\rangle \langle 0, \varepsilon_{01}| \\ & + (p_1 - p_2) \alpha\beta^* |1, \varepsilon_{00}\rangle \langle 0, \varepsilon_{01}| + (p_1 - p_2) \alpha^*\beta |0, \varepsilon_{01}\rangle \langle 1, \varepsilon_{00}|, \end{aligned} \quad (21)$$

which can be rewritten in the orthogonal basis $\{|0, \varepsilon_{00}\rangle, |1, \varepsilon_{01}\rangle, |1, \varepsilon_{01}\rangle, |0, \varepsilon_{01}\rangle\}$,

$$\rho'' = \begin{pmatrix} (p_0 + p_3) |\alpha|^2 & (p_0 - p_3) \alpha\beta^* & 0 & 0 \\ (p_0 - p_3) \alpha^*\beta & (p_0 + p_3) |\beta|^2 & 0 & 0 \\ 0 & 0 & (p_1 + p_2) |\alpha|^2 & (p_1 - p_2) \alpha\beta^* \\ 0 & 0 & (p_1 - p_2) \alpha^*\beta & (p_1 + p_2) |\beta|^2 \end{pmatrix}, \quad (22)$$

with

$$p_0 + p_1 + p_2 + p_3 = 1. \quad (23)$$

The information I_0 that Eve can get is equal to the Von Neumann entropy

$$I_0 = -\sum_{i=0}^3 \lambda_i \log_2 \lambda_i. \quad (24)$$

Where $\lambda_i (i = 0, 1, 2, 3,)$ are the eigenvalues of ρ'' , which are

$$\begin{aligned} \lambda_{0,1} &= \frac{1}{2}(p_0 + p_3) \pm \frac{1}{2} \sqrt{(p_0 + p_3)^2 - 16p_0p_3|\alpha|^2|\beta|^2} \\ &= \frac{1}{2}(p_0 + p_3) \pm \frac{1}{2} \sqrt{(p_0 + p_3)^2 - 16p_0p_3(d - d^2)} \end{aligned} \quad (25)$$

$$\begin{aligned} \lambda_{2,3} &= \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2} \sqrt{(p_1 + p_2)^2 - 16p_1p_2|\alpha|^2|\beta|^2} \\ &= \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2} \sqrt{(p_1 + p_2)^2 - 16p_1p_2(d - d^2)} \end{aligned} \quad (26)$$

In the case of $p_0 = p_1 = p_2 = p_3 = 0.25$, where Alice encodes exactly 2 bits, expression(25-26) simplify to $\lambda_0 = 0.5d, \lambda_1 = 0.5(1 - d), \lambda_2 = 0.5d$ and $\lambda_3 = 0.5(1 - d)$. Interestingly, the maximal information gain is equal to the Shannon entropy of a binary channel

$$I_0(d) = -\frac{1}{2}d \log_2\left(\frac{1}{2}d\right) - \left(\frac{1}{2} - \frac{1}{2}d\right) \log_2\left(\frac{1}{2} - \frac{1}{2}d\right)$$

$$-\frac{1}{2}d \log_2(\frac{1}{2}d) - (\frac{1}{2} - \frac{1}{2}d) \log_2(\frac{1}{2} - \frac{1}{2}d). \quad (27)$$

Then assume that Bob sends $|1\rangle$ rather than $|0\rangle$. The above security analysis can be done in full analogy, resulting in the same crucial relations. The maximal amount of information is equal to the Shannon entropy of a binary channel

$$\begin{aligned} I_1(d) = & -\frac{1}{2}d \log_2(\frac{1}{2}d) - (\frac{1}{2} - \frac{1}{2}d) \log_2(\frac{1}{2} - \frac{1}{2}d) \\ & -\frac{1}{2}d \log_2(\frac{1}{2}d) - (\frac{1}{2} - \frac{1}{2}d) \log_2(\frac{1}{2} - \frac{1}{2}d). \end{aligned} \quad (28)$$

So the maximal amount of information that Eve can obtain is

$$I = \frac{1}{2}(I_0 + I_1) = 1 - d \log_2 d - (1 - d) \log_2(1 - d). \quad (29)$$

After some simple mathematical calculations in FPP, when $a = t$, get

$$d_{lF} = 1 - a^3, \quad (30)$$

and the maximum I is

$$I(d_{lF}) = 1 + H(\sqrt[3]{1 - d_{lF}}), \quad (31)$$

where

$$H(x) = -x \log_2 x - (1 - x) \log_2(1 - x). \quad (32)$$

However, in DPP, the maximum I is

$$I(d_{lD}) = 1 - d_{lD} \log_2 d_{lD} - (1 - d_{lD}) \log_2(1 - d_{lD}) = 1 + H(d_{lD}). \quad (33)$$

The above analysis shows that function $I(d_{lD})$ and $I(d_{lF})$ have the similar algebraic properties. If Eve wants to gain the full information ($I = 2$), the probabilities of eavesdropping detection are $d_{lD}(I = 2) = 0.5$ in DPP and $d_{lF}(I = 2) = 0.88$ in FPP.

In order to contrast the two functions, Fig.2 is given. As are shown in Fig.2, if Eve wants to gain the full information, she must face a larger detection probability in FPP than DPP. This also indicates that FPP is more secure than DPP.

Taking into account the probability c of the decoy mode, the effective transmission rate, i.e. the number of message bits per protocol run, is $1 - c$, which is equal to the probability for a message transfer. So, if Eve wants to eavesdrop one message transfer without being detected, the probability for this event is

$$s(c, d) = (1 - c) + c(1 - d)(1 - c) + c^2(1 - d)^2(1 - c) + \dots = \frac{1 - c}{1 - c(1 - d)}. \quad (34)$$

Then the probability of successful eavesdropping $I = nI(d)$ bits is $s(I, c, d) = s(c, d)^{I/I(d)}$. So

$$s(I, c, d) = \left(\frac{1 - c}{1 - c(1 - d)} \right)^{I/I(d)}, \quad (35)$$

where

$$I(d) = 1 + H(\sqrt[3]{1-d}). \quad (36)$$

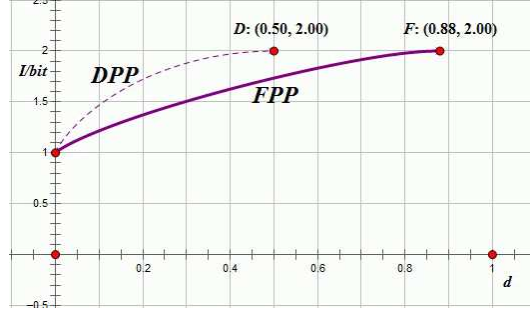


Fig. 2. The comparison of the two detection results. The dotted line expresses the function $I(d_{ID})$ in DPP and the thick line expresses the function $I(d_{IF})$ in FPP. Obviously, if Eve wants to get the full information, she must encounter the higher detection efficiency in FPP

Now let us analyze the security of the FPP. In the limit $I \rightarrow \infty$ (a message or key of infinite length) get $s \rightarrow 0$, so the presented protocol in this paper is *asymptotically secure*. If the security of the quantum channel is ensured, the protocol is completely secure. For example, a choice of the decoy mode is $c = 0.5$. In Fig.3, the eavesdropping success probability as a function of the information gain I is plotted, for $c = 0.5$ and for different detection probabilities d which Eve can choose. Note that for $d < 0.5$, Eve only gets part of the message right and does not even know which part. So, the FPP protocol is proved secure.

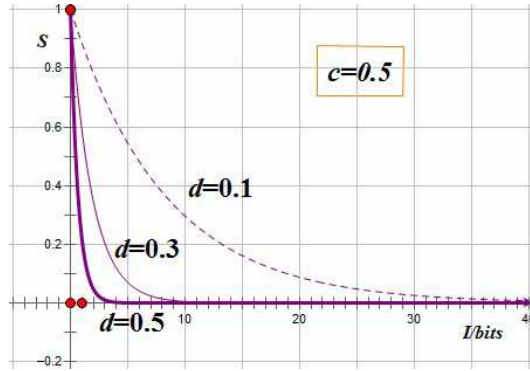


Fig. 3. Eavesdropping success probability as a function of the maximal eavesdropped information, plotted for different detection probabilities d .

4 Conclusion and Further Work

In summary, an improved eavesdropping detection strategy based on quantum direct communication protocol based on four-particle GHZ state has been introduced, and two eavesdropping detection strategies are compared quantitatively by using the constraint between the information that eavesdropper obtains and the interference introduced. In FPP, the sequence B is always in hands of Bob and Eve can only touch the sequence A , and any useful message will not be leaked to the potential eavesdropper. So the security message can be securely transmitted to the receiver. Compared with the DPP, in the FPP protocol, the four-particle GHZ state particles are used to detect eavesdropping which increases the efficiency of detection eavesdropping.

In the analysis, if the eavesdropper obtains the full information, she must face a larger detection probability in the FPP than DPP, which shows that the efficiency of eavesdropping detection in FPP is higher than DPP, so it can ensure the quantum direct communication protocol more secure. In order to detect eavesdropping, Bob sends more decoy photons than DPP, while this method reduces the number of measurement. That is, Bob gains the better security at the cost of sending more particles.

As we know, the quantum direct communication protocol can also be used as an efficient QKD protocol. In this paper, only the situation that the improved protocol is used as a QKD strategy is considered. So the weaknesses which the quantum direct communication protocol must be faced, such as the noise channel [39-40], the Dos attack [41-42] and so on, may not be considered. In the further work, the other QSDC protocol will be researched.

References

- [1] C. H. Bennett, G. Brassard, In: International Conference of Computers in Systems and Signal Processing, Dec, 1984, Bangalore, India (IEEE, New York 1984) 175
- [2] C. H. Bennett, G. Brassard, C. Crepeau et al., Phys. Rev. Lett. 70, 1895 (1992)
- [3] D. Bouwmeester, J. W. Pan, K. Mattle et al., Nature 390, 575 (1997)
- [4] D. Bouwmeester, K. Mattle, J. W. Pan et al., Appl. Phys. B-Lasers 67, 749 (1998)
- [5] K. Yooh-Ho, S. P. Kulik, S. Yanhua, In: Quantum Electronics and Laser Science Conference, May 6-11, 2001, Baltimore, MD(Opt. Soc. America, 2001) 223
- [6] P. Hari, In: International Conference on Emerging Trends in Electronic and Photonic Devices & Systems, Dec 22-24, 2009, India (IEEE, New York, 2009) 18

- [7] F. Akira, In: Quantum Electronics and Laser Science Conference, May 16-21, 2010, San Jose, CA(IEEE, New York 2010) 223
- [8] C. H. Bennett, S. J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992)
- [9] M. Klause, H. Weinfurter, G. K. Paul et al., Phys. Rev. Lett., 76, 25 (1996)
- [10] M. Hillery, V. Buzek, A. Berthiaume, Phys. Rev. A 59, 1829 (1999)
- [11] R. Cleve, D. Gottesman, H. K. Lo, Phys. Rev. Lett. 83, 648 (1999)
- [12] K. Shimizu, N. Imoto, Phys. Rev. A 60, 157 (1999)
- [13] K. Shimizu, N. Imoto, Phys. Rev. A 62, 054303 (2000)
- [14] A. Beige, B. G. Englert, C. Kurtsiefer et al., Acta. Phys. A 101, 357 (2002)
- [15] F. G. Deng, G. L. Long, Phys. Rev. A 69, 052319 (2004)
- [16] Q. Y. Cai, B. W. Li, Chin. Phys. Lett. 21, 601 (2004)
- [17] M. Lucamarini, S. Mancini, Phys. Rev. Lett. 94, 140501 (2005)
- [18] F. G. Deng, G. L. Long, X. S. Liu, Phys. Rev. A 68, 042317 (2003)
- [19] Q. Y. Cai, B. W. Li, Phys. Rev. A 69, 054301 (2004)
- [20] T. Gao, F. L. Yan, Z. X. Wang, Chin. Phys. Lett. 22, 2473 (2005)
- [21] C. Wang, F. G. Deng, G. L. Long, Opt. Commun. 253, 15 (2005)
- [22] X. H. Li, F. G. Deng et al., Phys. Rev. A 74, 054302 (2006)
- [23] X. H. Li, C. Y. Li, F. G. Deng et al., Chin. Phys. Lett. 16, 2149 (2007)
- [24] B. A. Nguyen, Phys. Lett. A 328, 6 (2004)
- [25] Z. X. Man, Z. J. Zhang, Y. Li, Chin. Phys. Lett. 22, 22 (2005)
- [26] X. Ji, S. Zhang, Chin. Phys. Lett. 15, 1408 (2006)
- [27] Z. X. Man, Y. J. Xia, B. A. Nguyen, J. Phys. B-At. Mol. Opt. Phys. 39, 3855 (2006)
- [28] Z. X. Man, Y. J. Xia, Chin. Phys. Lett. 23, 1680 (2006)
- [29] Y. Xia, C. B. Fu. S. Zhang et al., J. Korean Phys. Soc. 48, 24 (2006)
- [30] X. R. Jin, X. Ji, Y. Q. Zhang et al., Phys. Lett. A 354, 67 (2006)
- [31] Z. X. Man, Y. J. Xia, Chin. Phys. Lett. 24, 15 (2007)
- [32] Y. Chen, Z. X. Man, Y. J. Xia, Chin. Phys. Lett. 24, 19 (2007)
- [33] Y. G. Yang, Q. Y. Wen, Sci. China Ser G-Phys. Mech. Astron 50(5), 558 (2007)
- [34] K. Bostrom, T. Felbringer, Phys. Rev. Lett. 89, 187902 (2002)

- [35] G. Brassard, L. Salvail, LNCS 765, 410 (1994)
- [36] G. L. Long, X. S. Liu, Phys. Rev. A 65(3), 032302 (2002)
- [37] C. Y. Li, H. Y. Zhou, Y. Wang et al., Chin. Phys. Lett. 22(5), 1049 (2005)
- [38] C. Y. Li, X. H. Li, F. G. Deng et al., Chin. Phys. Lett. 23(11), 2897 (2006)
- [39] A. Wojcik, Phys. Rev. Lett. 90(15), 157901 (2003)
- [40] F. G. Deng, X. H. Li, C. Y. Li et al., Chin. Phys. Lett. 16, 277 (2007)
- [41] Q. Y. Cai, Phys. Rev. Lett. 91, 109801 (2003)
- [42] Z. J. Zhang, Z. X. Man, Int. J. Quantum Inf. 2, 521 (2004)